




THE DEPUTY SECRETARY OF THE INTERIOR
WASHINGTON

JUN 15 2015

Memorandum

To: All Department of the Interior Employees

From: Deputy Secretary 

Subject: Follow-up on the Cybersecurity Incident

I am writing to provide you an update on the ongoing investigation into the cyber intrusion at the U.S. Office of Personnel Management (OPM) announced on June 4, 2015. The OPM has recently discovered that additional systems were compromised. These systems included those that contain information related to the background investigations of current, former, and prospective Federal Government employees, as well as other individuals for whom a Federal background investigation was conducted.

This separate incident – like the one that was announced on June 4 affecting personnel information of current and former Federal employees – was discovered as a result of OPM's aggressive efforts to update its cybersecurity posture, adding numerous tools and capabilities to its network.

The OPM, the Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI) are working as part of this ongoing investigation to determine the number of people affected by this separate intrusion. The OPM will notify those individuals whose information may have been compromised as soon as practicable. You will be updated when we have more information on how and when these notifications will occur.

The OPM remains committed to improving its security capabilities and has invested significant resources in implementing tools to strengthen its security barriers. Additionally, OMB has instructed Federal agencies to immediately take a number of steps to further protect Federal information and assets and improve the resilience of Federal networks. We are working closely with OMB, DHS, and other experts across the Government in these efforts to detect and thwart evolving and persistent threats, and ensure that the Department of the Interior is able to deliver its mission of protecting America's natural resources and heritage, honor our cultures and tribal communities, and supply the energy to power our future.

As we have recently shared with you, the following are some key reminders of the seriousness of cyber threats and of the importance of vigilance in protecting our systems and data.

Steps for Monitoring Your Identity and Financial Information

- Monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.
- Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. Consumers are entitled by law to one free credit report per year from each of the three major credit bureaus – Equifax[®], Experian[®], and TransUnion[®] – for a total of three reports every year. Contact information for the credit bureaus can be found on the Federal Trade Commission (FTC) website, www.ftc.gov.
- Review resources provided on the FTC identity theft website, www.Identitytheft.gov. The FTC maintains a variety of consumer publications providing comprehensive information on computer intrusions and identity theft.
- You may place a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Simply call TransUnion[®] at 1-800-680-7289 to place this alert. TransUnion[®] will then notify the other two credit bureaus on your behalf.

Precautions to Help You Avoid Becoming a Victim

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues, or any other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, <http://www.us-cert.gov/ncas/tips/ST04-013>).
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (<http://www.antiphishing.org>).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls, <http://www.us-cert.gov/ncas/tips/ST04-004>; Understanding Anti-Virus Software, <http://www.us-cert.gov/ncas/tips/ST04-005>; and Reducing Spam, <http://www.us-cert.gov/ncas/tips/ST04-007>).
- Take advantage of any anti-phishing features offered by your email client and web browser.

- Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.
- Additional information about preventative steps by consulting the Federal Trade Commission's website, www.consumer.gov/idtheft. The FTC also encourages those who discover that their information has been misused to file a complaint with the commission using the contact information below.
- For more information, contact the Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580
<https://www.identitytheft.gov> 1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502